WTF? Locating Performance Problems in Home Networks

Srikanth Sundaresan*, Yan Grunenberger†, Nick Feamster*, Dina Papagiannaki†, Dave Levin‡, Renata Teixeira∓
* Georgia Tech † Telefonica I+D ‡ University of Maryland ∓ LIP6

ABSTRACT

Most users of home networks have experienced the intense frustration that comes with diagnosing poor performance. Even determining something as simple as whether a performance problem lies with the ISP or somewhere in the home network is incredibly difficult; this lack of visibility results in unnecessary service calls to ISPs and a general inability to have the network perform as well as it should. In this paper, we design and develop *WTF (Where's The Fault?)*, a system that reliably determines whether a performance problem lies with the user's ISP or inside the home network. The tool can also distinguish these problematic situations from the benign case when the network is simply under-utilized. WTF uses cross-layer techniques to discover signatures of various pathologies. We implemented WTF in an off-the-shelf home router; evaluated the techniques in controlled lab experiments under a variety of operating conditions; validated it in real homes where we can directly observe the home conditions and network setup; and deployed it in 30 home networks across North America. The real-world deployment sheds light on common pathologies that occur in home networks. We find, for instance, that many users purchase fast access links but experience significant (and frequent) performance bottlenecks in their home wireless network.

1. INTRODUCTION

A typical user's Internet access passes through the home wireless network, the access link, and the access ISP's network before heading to points beyond. Home network users commonly experience the consequences of a poorly performing Internet connection, which include slow-loading Web pages, poor-quality or dropped VoIP calls, or buffering during streaming video sessions. These pathologies are readily evident and highly frustrating for users; yet, they are equally difficult to diagnose. A user may have difficulty determining why a problem is occurring, but also *where* it is occurring. As frustrated as users are by these problems, Internet service providers (ISPs) are equally frustrated: Our discussions with several large access ISPs reveal that service calls are costly, ranging from $9–25 per call, and as many as 75% of service calls from customers are usually caused by problems that have nothing to do with the ISP. Hence, both users and ISPs could benefit from techniques that could better isolate performance problems in home networks. Even simply being able to determine whether the problem was inside the home network or elsewhere would be a reasonable starting point.

Performance problems in home networks have many possible causes. *Inside the home*, problems can result from a bad wireless connection, caused by poor placement of the access point or the end host, interference from other access points, or end hosts within the same network. Cross traffic from other devices on the network might also reduce the capacity of the wireless network. The end host might be the cause of problems if it cannot cope with application traffic, or if the network interface or driver is somehow faulty. *Outside the home*, a shaped or lossy access link, routing problems within ASes, poor interconnectivity between ASes in the path, a high latency path to the server, or even a poorly optimized server can all introduce bottlenecks. Most of the time, the ends of a network path (the user or the application provider) have only a limited view of the network; in most common practical cases, tools running at network endpoints path cannot effectively localize problems beyond the immediate next hop. Application providers can sometimes identify that clients are experiencing poor performance, but they typically have no visibility into why the performance is poor.

In this paper, we develop a tool called *WTF, (Where's The Fault?)* that localizes performance problems that users experience in home networks to the home wireless network, the access link, or the application. WTF builds on the intuition that, given enough traffic demand from users and applications in the home network, a path out of the home network will typically either have a bottleneck on the access link or inside the home network. WTF offers this granularity of information, which can better inform users about how to improve the performance of their home network (*e.g.*, upgrading their service plan, fixing the wireless network). We deploy WTF in the home access point, which allows it to directly observe the access link and the local wireless network on path. WTF passively monitors the network performance characteristics of real user traffic across multiple layers to determine which side of the access link is experiencing a bottleneck. This allows WTF to help the user ultimately drill down to a diagnosis; for example, WTF can determine whether the access link is throttling the TCP connection, whether the wide-area network is introducing TCP loss, and whether the home wireless network is introducing a bottleneck. In one of our deployments of a user with a high-end service, for example, WTF detected extremely low bitrates and high link-level retransmissions, creating a bottleneck in the user's home wireless network (further investigation in this particular home found the user's wireless access point tucked away in the closet).

WTF collects a variety of statistics across network protocol layers and uploads them to a central server that analyzes

the measurements. Although WTF does not determine *why* a bottleneck exists, we believe that the level of localization that WTF provides represents an important step for diagnosis (as evidenced by users' floods of service calls to ISPs for problems that often lie within the home). Because WTF's heuristics rely on various operational details of TCP, the tool can currently only localize bottlenecks for TCP flows.

Our goal of continuous monitoring in real home networks requires us to deploy analysis software on existing home network infrastructure—specifically the home router/access point. Because this vantage point is located on the path at a "demarcation point" between the home network and the access link, it provides a unique opportunity to observe performance characteristics on each side of the device, thereby making it easier to localize performance problems to either inside or outside the home. It also has the advantage of being a device that every home network user deploys, and it typically remains on all of the time, making it easy to gather continuous measurements. Unfortunately, deploying at this vantage point also introduces CPU, memory, and network constraints that impose additional constraints and challenges on WTF's design.

We implemented WTF as custom firmware that runs on an off-the-shelf home router; the tool collects passive measurements, pre-processes the data, and uploads it to a server for analysis. To validate WTF, we perform extensive controlled laboratory experiments; we also analyze WTF's measurements in five homes by running additional tests, and studying both user traffic demands and the home wireless setup in those homes. We then deploy WTF in 30 homes across North America and report on the extent of wireless and access network performance problems that users experience in these networks over the course of 9–21 days.[1]

Our study yields some interesting findings: notably, most homes in our deployment have wireless problems most of the time, and are likely bottlenecked by the wireless network. In many cases, the performance of the wireless network is so bad that the round-trip latency introduced by the wireless network may be a significant fraction of the end-to-end round-trip latency (at least for users in North America where services are often located close to users). Thus, in addition to the significant attention that is already being paid to optimizing wide-area performance and host TCP connection settings, our results suggest that it is worth spending effort to improve home wireless network performance. The next steps should be to understand the underlying causes of poor wireless performance (*e.g.*, the nature of interference and contention in home wireless networks).

The rest of the paper is structured as follows. Section 2 develops the ideas and intuition behind WTF and describes and evaluates them in a controlled lab setting in detail. Section 3 describes our prototype implementation, and Section 4 evaluates the performance of our system under different condition in five homes. Section 5 reports on the state of the home network as seen from 30 homes in the deployment.

[1] Although deploying across more home networks will yield more general results, deploying WTF for this study required university institutional review board (IRB) approval, which slowed our recruitment process. We have recently received clearance to deploy WTF more widely.

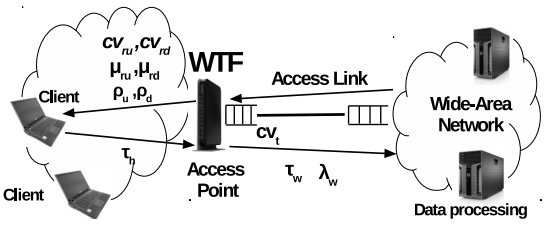


Figure 1: *The general home network setup, and the parameters that WTF measures. WTF runs on the access point between the home network and the access link, thus offering a unique vantage point for observing pathologies on either side.*

2. LOCATING PERFORMANCE PROBLEMS

Home networks can induce performance problems for TCP connections for a variety of reasons. Our goal is to develop methods and heuristics to localize these pathologies as being either in the home network or elsewhere, and to provide additional details about the reasons for the pathology, if possible. WTF aims to distinguish between three scenarios: (1) the access link is the bottleneck, (2) the wireless link is the bottleneck; and (3) the demand on the network is not enough to saturate either the access link or the wireless link (*e.g.*, due to insufficient flow lengths, high latency paths, or loss in the wide area network). We first describe the problem setup and the intuition behind WTF's heuristics. Then, we explain our approach to validating these heuristics, including the setup for our controlled experiments.

2.1 Problem and Approach

Setup and intuition. Figure 1 shows how a typical home network connects to the wide-area Internet, and places where WTF collects various performance metrics. Table 1 summarizes the performance metrics that WTF collects. WTF captures and analyzes traffic traces over short periods, about one second. This measurement frequency is typically sufficient to capture hundreds of packets and frames, depending on the capacity of the access link.

Overview of WTF approach. First, WTF determines whether the access link is a bottleneck by exploiting properties of how TCP congestion control interacts with bottleneck links. Second, WTF analyzes the wireless network to look for a suite of features derived from bitrate adaptation and its effects on TCP. A set of lightweight heuristics identifies the wireless network as the cause of the problem if various characteristics are detected. Finally, WTF scrutinizes TCP traces for evidence of loss or of high latency paths. If none of the

Parameter	Description	Role
cv_t	Co-efficient of variation of interpacket arrival time	Detects access link bottleneck
cv_{ru},cv_{rd}	Upstream and downstream co-efficient of variation of 802.11 frame bitrate	Suggests varying/poor channel
μ_{ru},μ_{rd}	Up. and down. avg. bitrate of frames normalized by max. bitrate supported	Suggests poor channel
ρ_u,ρ_d	Up. and down. frame retransmission rates	Suggests lossy channel
τ_h	TCP RTT between the AP and the client	Suggests contention, and/or wireless bandwidth bottleneck
τ_w	TCP RTT between the AP and the server	Suggests high latency link
λ_w	Fraction of triple-duplicate ACKs in TCP connections	Suggest loss in the end-to-end connection

Table 1: *The components that WTF measures and the roles that they play in helping localize faults to either the home network or the access link.*

features can positively identify the source of the problem, WTF infers that the network must have insufficient demand to saturate the bottleneck link. The algorithm has three steps:

1. **Determine whether the access link is a bottleneck.** WTF first determines whether the access link is bottlenecked or not, by computing the coefficient of variance of packet inter-arrival time, cv_t, and comparing it against a threshold (in Section 2.2, we describe how we set these thresholds). While values much lower than the threshold increase the confidence of the deduction, WTF only uses a binary decision process, in order to avoid parameter tuning.
2. **Look for pathologies in the wireless network.** WTF analyzes 802.11 frames for different parameters for estimating the quality of the wireless link; cv_{ru} and cv_{rd}, the coefficient of variation of the upstream and downstream bitrates, μ_{ru} and μ_{rd}, the normalized average upstream and downstream bitrates, ρ_u and ρ_d, the retransmission rates. From TCP traces, it computes τ_h, the TCP RTT over the wireless network. If any of these parameters breach the specified threshold, WTF flags the wireless as a potential bottleneck.
3. **Look for pathologies in the wide-area.** If either the TCP loss parameter λ_w, or the TCP RTT to the server (τ_w) are high, WTF deduces that the wide-area network is potentially introducing the bottleneck.

If none of the above conditions hold (the access link is not saturated, and there is no obvious bottleneck on the wireless link or the wide-area network), WTF deems that there is insufficient demand on the access link. Wireless and wide-area bottlenecks are usually only a problem if they prevent full use of the access link; if the access link is being throttled anyway (which is likely in cases where the access capacity is low), then the wireless and access link performance problems are not likely to matter.

2.2 Validating WTF's Heuristics

In this section, we explain how we validate each of WTF's diagnosis heuristics using controlled experiments. We also describe empirical measurements that we use to justify the settings of the thresholds for each parameter.

2.2.1 Experiment setup

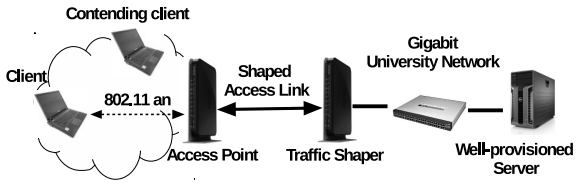
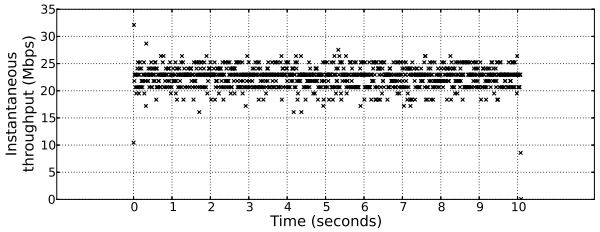


Figure 2: *Controlled experiment setup.*

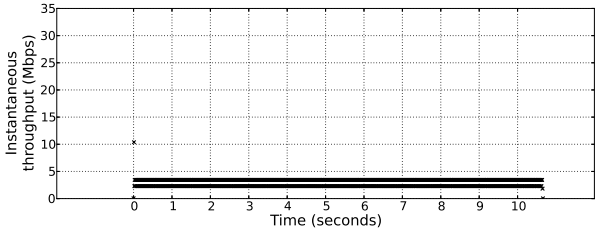
We build a controlled testbed to evaluate the components of WTF. The test bed consists of an access point, the associated LAN, a network shaper upstream of the access point, a well provisioned university network, and servers in the university network. The access point is a Netgear WNDR3800 router running a version of OpenWrt. Figure 2 shows a schematic of this experimental setup.

Downstream of the access point, connected to the access point over a 802.11 network (both a and n are evaluated), are one or two end-hosts (depending on the experiment). We run our experiments in the 5 GHz spectrum, which is less polluted than the 2.4 GHz spectrum in our lab. The network shaper is another Netgear WNDR3800 router running OpenWrt. We perform network traffic shaping with `tc` and `netem`. We adjust the bandwidth, latency, and loss of the emulated access link. The shaper is located physically close to the first access point where it also captures wireless traffic; it has a similar radio as the access point. This allows us to obtain ground truth concerning wireless network conditions when we try to induce wireless pathologies such as weak signal strength and frame drops. Upstream of the shaper is a well-provisioned university network. We run our controlled experiments against servers in this network to minimize the likelihood that bottlenecks lie elsewhere on the end-to-end path. We induce wireless pathologies using a different set of techniques. First, we reduce the transmission power of the access point and move the clients to different distances from the access point. This approach allows us to measure performance under different wireless channel conditions, but without any guarantees on the throughput or the loss of the channel. We evaluate channel contention using a second laptop and running an iperf UDP session from the access point at different rates.

2.2.2 Access link bottleneck detection



(a) *Wireless link bottleneck. Instantaneous throughput at the wide-area interface varies at short time scales due to high variance in packet inter-arrival times.*



(b) *Access link bottleneck. Instantaneous throughput at the wide-area interface is steady, due relatively uniform packet inter-arrival times caused by upstream shaping.*

Figure 3: *Behavior of packet inter-arrival times when the access-link is the bottleneck, and when it is not.*

WTF can compute the bandwidth of flows by capturing all flows at the access point, yet it is more difficult to identify whether the achieved throughput is throttled by a capacity constrained link in the path, or by other factors such as loss, or the application generating the traffic. We begin by analyzing whether the access link is a bottleneck. To do so, we utilize the following property of bottleneck links: since the bottleneck link services packets at a rate slower than they arrive, queues build up at the head of the link, and the access link sends packets at a fairly even rate. The natural variation in packet inter-arrival times caused by TCP effects (*e.g.*, the classical "saw-tooth" effect) are seen only upstream of the bottleneck link but not downstream.

Figures 3a and 3b illustrate this effect. The figures show the throughput of a TCP connection at the WAN port of the access point, at 10 ms granularity. In Figure 3a, the access link is at 100 Mbps, and the wireless link is 802.11a, with a clean channel. The wireless link is obviously the bottleneck here, as the maximum TCP rate it can support is less than 100 Mbps (about 21 Mbps in this case). We see the variation in instantaneous throughput effect caused by congestion control. Figure 3b shows the case where the access link is the bottleneck. Here, the access link is shaped to 3 Mbps, while the wireless link is not modified. We see from the throughput plots that, as expected, the wireless is not the bottleneck, and there is very little variation in the throughput.

The above example shows an extreme case, but it offers a feature, which we exploit to identify whether the access link is the bottleneck: packet inter-arrival times at the WAN interface. We expect to see high variance in the packet inter-arrival times before the bottleneck link due to congestion control, but significantly lower variance after the bottleneck link itself because of the buffer's smoothing effect. Therefore, to identify whether the access link is shaping traffic,WTF applies a single threshold for cv_t, which is the coefficient of variation of the inter-packet arrival time at the WAN port of the access point. The threshold checks whether the variance of the packet inter-arrival times at the WAN interface is high compared to the average. If the variance factor is lower than the threshold, then we identify the access link as the bottleneck; in our controlled measurements, we explore how to set this threshold.

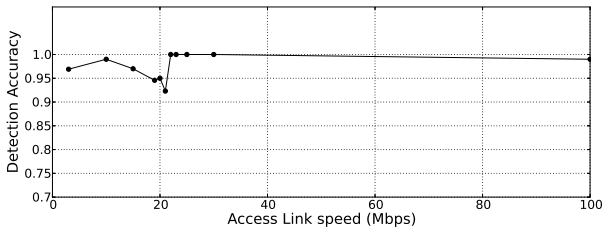
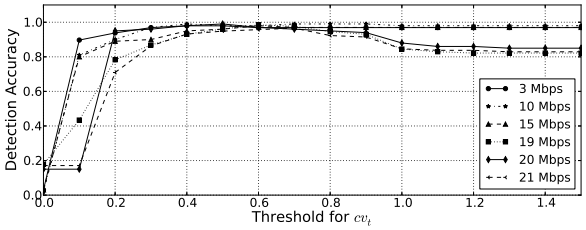
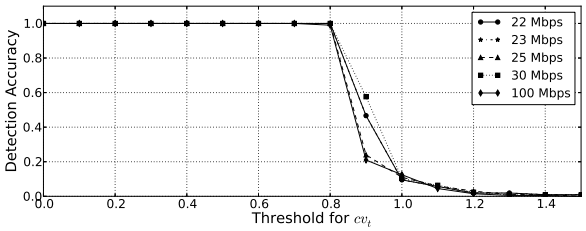


Figure 4: *Detection accuracy with the wireless channel held constant at about 21 Mbps. Detection accuracy is high except when the access link speed is similar to the wireless speed.*



(a) *For access link throughputs less than the wireless throughput, the lower bound is sensitive*



(b) *For access link throughputs greater than the wireless throughput, the upper bound is sensitive*

Figure 5: *Sensitivity of detection accuracy to threshold of cv_t. There is a wide range between the two extremes where detection accuracy is high.*

Validation We run two sets of experiments to evaluate the effectiveness of our algorithm in detecting bandwidth bottlenecks. We establish the maximum rate at which TCP can operate in the wireless settings, and then we test different access links speeds against the best possible wireless link. We evaluate the detection accuracy of the algorithm in this setting. We run this experiment 100 times for each access link speed setting.

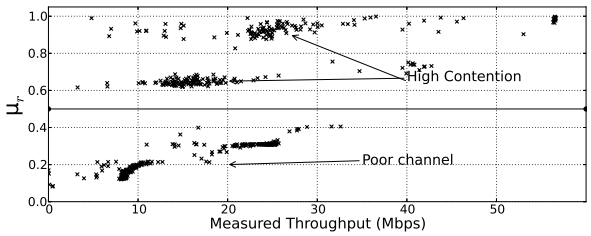
Figure 4 shows the results of this experiment. We see that

detection accuracy is generally quite high, in excess of 90% in all cases. The threshold value used here is 0.8. Detection accuracy drops when the access link is shaped at around 21 Mbps which is approximately the maximum speed of the wireless speed. In such cases, the capacity of the access link is close enough to the wireless capacity that the wireless could in fact be the bottleneck in some cases. As the wireless and the access link speeds converge, it may not even be meaningful to try label one side as the bottleneck due to natural variations. We see, however, that as the difference between the two sides increases, the detection accuracy is very close to 100%.

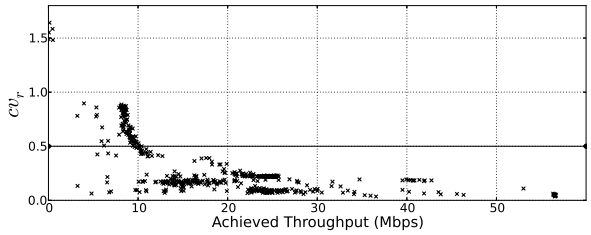
We now evaluate the robustness of the detection threshold for different threshold values for cv_t. Figure 5 shows the results. The cv_t represents the coefficient of variation of the packet inter-arrival time at the WAN interface of the access point. When the threshold is low (close to zero), it will always identify the wireless as the bottleneck, and when it is too high, it will always identify the access link as the bottleneck.

The results indicate that detection accuracy remains high for a wide range of threshold settings. When the access link is the bottleneck, the coefficient of variation is low, of the order of about 0.2, and when the wireless is the bottleneck, it is above 0.8, across a wide range of network conditions. This makes a robust value of the threshold easy to determine. In the case where the wireless link and the access link are close to each other in capacity, we see that cv_t falls somewhere in between (detection accuracy is high between about 0.5 and 0.8). Although we use a binary decision to denote the access link as a bottleneck based on a single threshold, we note that middling values denote an operating regime where accurately detecting a bottleneck is difficult.

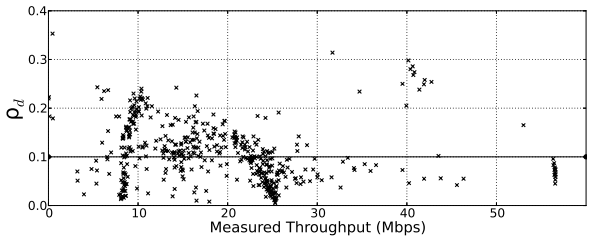
Applying the cv_t parameter in real networks. This technique relies on the access link shaping packets to work. If the access link is saturated, then *all* flows coming into the home network will be spaced out, so it does not rely on per flow spacing. Prior work [20] has used similar techniques to cluster flows that share bottleneck links by clustering flows that minimize entropy of packet inter-arrival time; the assumption being that bottleneck link reduces the entropy in packet inter-arrival times. The experiments in the previous section study the case when either the access link or the wireless link is the bottleneck. In a real home network, though, if the access link is not the bottleneck, then it could be the wireless, or it could be that there simply isn't sufficient demand to saturate either the access link or the wireless. It is not straightforward to differentiate between the two cases; all we can say using this technique is when the access link is *not* the bottleneck. WTF circumvents this problem by only considering cases when it sees a minimum amount of traffic in the network (100 packets/second). Real home networks also could have access link speeds varying over short-term intervals [30]. With PowerBoost [9] and other shaping techniques, throughput can drop significantly over the course of a few seconds. WTF deals with this by only considering traffic over one-second intervals. It is unlikely that link speeds change considerably over that time interval when there is sufficient demand. To eliminate the wireless as the source of the bottleneck, WTF uses wireless measurements as explained in Section 2.2.3. If the wireless is not the problem, then by default WTF assumes that there is not enough demand to saturate the network. If the upstream link is also wireless (*e.g.*, WiMAX), this technique may not work due to variation in the packet inter-arrival times. When there is heavy upstream traffic that saturates the upstream connection, the ACKs that traverse the downstream path will be evenly spaced. We avoid this by only considering cases with significant downstream traffic. We leave these cases for future work.



(a) *Normalized average bitrate. Lower values of μ_r indicates poor channel. However, a channel with high contention (therefore lower per-client capacity) could have high values of μ_r. We set the detection threshold to 0.5.*



(b) *Coefficient of variation of bitrate. Poor channel leads to higher variation of bitrates, therefore higher cv_r. We set the detection threshold to 0.5.*



(c) *Retransmission rate at different measured TCP throughput. Higher rates indicate poor channel. We set detection thresholds for ρ_u and ρ_d to 0.1.*

Figure 6: *Using bitrate adaptation to infer channel quality.*

2.2.3 Wireless bottleneck detection

We develop heuristics that evaluate the state of the wireless network. Wireless problems in home networks are varied; they could be caused due to poor connectivity, lossy channel, contention, or interference. We aim to determine whether the wireless network contributes to poor performance (which we

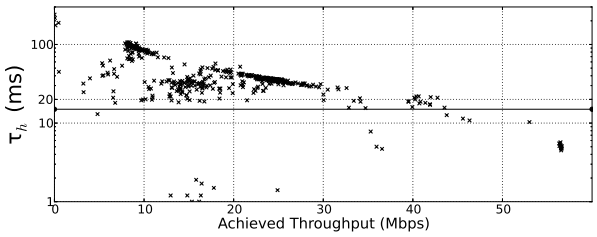


Figure 7: *TCP RTT between client and access point. λ_h decreases exponentially with higher throughput, regardless of cause of reduced throughput. We set detection threshold to 10 ms.*

declare to be the case when the wireless link is the bottleneck link in the end-to-end path) but do not concern ourselves with underlying causes of poor wireless performance.

WTF collects its measurements from a single vantage point: the access point. Although this approach has many limitations—notably, a single vantage point prevents identifying certain classes of problems such as hidden terminals—it has many advantages, especially because it allows us passively monitor traffic and apply cross-layer techniques such as correlating wireless and TCP parameters, to identify whether a problem exists. It enables wide deployment of the system in homes. We identify certain parameters that can be measured from the access point that provide good indications concerning the quality of the wireless network.

WTF uses these parameters to identify whether the wireless potentially has problems. For each of these parameters, WTF uses simple thresholds. The thresholds used are conservative (we also look at how it affects detection in later sections), and the purpose is to identify particularly egregious situations. WTF flags the wireless as problematic if *any* of the parameters breach the threshold. We motivate these parameters by running experiments with wireless pathologies and use these experiments to identify appropriate thresholds.

Bitrate adaptation. Bitrate adaptation techniques in IEEE 802.11 all vary the transmission bitrate in response to network conditions. Although these techniques usually adapt rates even under benign conditions to determine the channel quality, rate changes are usually rapid when the channel quality is poor. WTF computes retransmission rates and analyzes how the bitrates vary over time. Variation will be low if the channel quality is good, and high if the channel is poor or varying. Poor channels can still have stable bitrates if the protocol is able to find a (low) bitrate that is not lossy. We identify such cases by computing the average bitrate and normalizing it by the maximum bitrate supported by the protocol. For example, this would be 54 Mbits/s for 802.11 a/g.

We evaluate these techniques by running controlled experiments in a lab setting. We run two sets of experiments: (1) with the client at different distances from the access point; (2) with the client close to the access point, but contending for the channel with another client that sends constant UDP traffic. In the first case, we expect to observe many retransmissions and frame drops, and lower throughput. In the second case, we expect to see lower throughput, but higher bitrates (due to reasonable channel quality).

Figure 6a shows how the the *normalized bitrate* varies with achieved throughput. The figure shows two sets of points, one where the normalized average bitrate increases with achieved throughput, but only up to a certain level; this occurs when the channel is poor. This is the framerate adaptation algorithm in action, as it tries to search for an appropriate bitrate. In the latter case, the channel quality is good, but another client is contending for the channel. The second set of points is where the normalized average is uniformly high and independent of the throughput. Bitrate adaptation sees no reason to vary the bitrate in this case. We set a threshold of 0.5; if the normalized average is below this threshold, WTF recognizes the wireless as problematic. This setting weeds out the really bad cases of poor performance as shown in the figure.

Figures 6b shows how the *coefficient of variation of the bitrate* varies with the achieved throughput. As throughput increases, the coefficient reduces when the channel is poor, but it stays uniformly low when the channel is good but there is contention. This case is, in effect, an inverse of the normalized throughput case. We set a threshold of 0.5 here; if the coefficient of variation of the bitrate is higher than 0.5, WTF flags the wireless as pathological. This threshold is quite conservative as seen in the figure; with such high variance, it is unlikely that the wireless channel is good. In fact we see that with such a high bar, the throughput of connections that breach it have really low throughputs compared to what is achievable over the channel.

Retransmission rate. Figure 6c shows how the *downstream retransmission rate* varies with achieved throughput. In general, retransmissions are lower when the throughput is higher, because the channel is good. When the channel is bad and the throughput is low, we see that the retransmission rate varies widely because the channel sees dropped frames and bitrate adaptation attempts to reduce the bitrate. Sometimes, it succeeds and ultimately minimizes frame losses. Thus, although the retransmission rate can be a good indicator of wireless channel quality, it alone is not sufficient to determine the quality of the wireless channel. We use a threshold of 0.1 for this parameter; in general, from our experiments we see that this weeds out the cases where there is a significant throughput drop.

TCP round-trip time over wireless link. To isolate contented channels, WTF measures the TCP round-trip time between the access point and the client, of connections that pass through the access point. We analyze the traffic that passes through and extract the round-trip time component between the access point and the client, and the access point and the Internet server. Figure 7 shows how the local network RTT (between the access point and the client) varies as a function

of achieved throughput. We see that it decreases exponentially as a function of throughput. The RTT is independent of the cause of the pathology; both contention, and a poor channel result in high RTTs - of the order of tens of milliseconds. When there is no wireless bottleneck, the RTT can be expected to be quite low - of the order one millisecond, and not more than 4-5 ms. In this experiment, the access link is shaped to close to the maximum throughput achieved by the wireless channel. When there is a bottleneck in the wireless and everything else is fine, buffering delays in the driver and/or the LAN interface on the router can introduce high TCP RTTs as well. We set a threshold of 15 ms for the TCP RTT; such high RTTs are evidence that there are delays due to contention or buffering.

2.2.4 *Wide-area network pathologies*

Packet loss in the wide area on the end-to-end TCP connection can also create pathologies. This could be caused by the wireless connection, or outside the home. We analyze each TCP flow and check for the occurrence of triple-duplicate-acks (3dupacks). TCP uses 3dupacks as a signal that a packet has been lost, and retransmits that packet. WTF checks for the presence of 3dupacks in each flow, and if the fraction of the number of 3dupacks exceeds a certain threshold, it determines that the connection has experienced packet loss. This loss could have been caused either by conditions in the WAN or due to properties of the wireless network. We saw from our experiments that the fraction of 3dupacks in a TCP connection increases almost linearly with the loss rate of the connection grows. We are only interested in establishing whether the TCP connection experienced loss in the WAN, *not* in estimating loss rates. We therefore set a small non-zero threshold for the fraction of 3dupacks—if the fraction crosses this threshold, we establish that the connection saw a loss.

We evaluate the effectiveness of the algorithm in localizing loss on the access link with a good wireless link. For this experiment, we ensure that there is no loss in the wireless channel. We do this by analyzing the snooped wireless traces and weeding out cases where there were wireless frame drops. We use the fraction of 3dupacks (λ_w) to detect loss. Our experiments show that a low non-zero threshold is usually sufficient to detect lossy connections. Figure 8 shows the sensitivity of this threshold to packet loss: a low (or zero) threshold can detect lossy links. Since access networks do not often experience high loss rates [30], we are interested in capturing only cases where the loss is particularly high; WTF uses a threshold value if 0.02, which identifies loss of about about 3%. As we shall see in Section 5, only a small fraction of connections in our deployment see significant fractions of 3dupacks. In general, we do not observe regular evidence of wide-area packet loss that is significant enough to introduce performance bottlenecks.

Recall that WTF extracts the RTT between the access point and the wireless client; in a similar fashion, WTF can extract

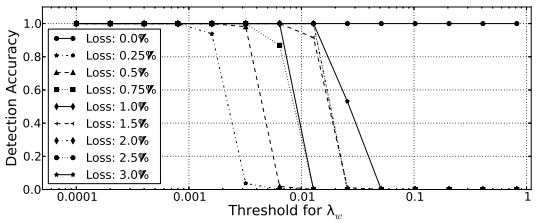


Figure 8: *Robustness of loss detection threshold with only access link losses.*

Parameter	Threshold	Conclusion
cv_t	≤ 0.8	Access link bottleneck.
cv_r	≤ 0.5	Possible poor wireless.
μ_r	≤ 0.5	Possible poor wireless.
ρ_u,ρ_d	≥ 0.1	Possibly lossy wireless.
τ_h	≥ 15 ms	Possible contention in wireless.
τ_w	≥ 100 ms	High latency.
λ_w	≥ 0.02	Loss in the wide area.

Table 2: *The threshold values that WTF uses for each parameter to detect pathologies.*

the RTT between the access point and the server in the wide-area network. This parameter, τ_w denotes the the round-trip latency between the access point and the content in the wide area. The throughput that TCP connections can achieve is inversely proportional to the latency. To account for this possibility, WTF uses a threshold of 100 ms to determine cases where content is particularly far from the access point. This threshold setting is specific to North America, where our deployment is located, but could be adjusted in other settings. Most popular content is progressively moving closer to access networks; in fact, we find that we see that only about 20% of TCP connections coming from home networks experience TCP round-trip times that exceed 100 ms.

3. WTF: PROTOTYPE IMPLEMENTATION

We describe a prototype of WTF, which we deploy in 30 locations (29 homes, and 1 university lab where it is used as a regular access point). We describe the design of the system and how we evaluate and validate it in five homes.

3.1 Design

We design and implement WTF to run on OpenWrt-equipped home access points. We use Netgear's WNDR3800 and 3700v2 routers. Both have an Atheros chipset with a 450 MHz processor, one 802.11gn radio, and one 802.11an radio. The driver used is ath9k and uses the minstrel rate adaptation algorithm. The 3800 has 128 Mbytes of RAM, and the 3700v2 has 64 Mbytes of RAM. All routers are equipped with an active measurement suite that measures upstream and downstream throughput approximately every two hours. Due to engineering challenges that resource limitations on the gateway introduce, the current prototype version of WTF does not run continuously; it collects data about every 5 minutes on average. It runs for 15 seconds every iteration. It then does partial pre-processing and anonymization

of the data on the router itself, and then uploads a compressed digest of the data to a server.

Sampling the data, rather than continuous monitoring, has advantages and disadvantages. Sampling allows us to reduce computation and storage and also facilitates for rapid development and deployment, since the software is running on commodity home routers. The measurements provide insight into the overall nature of each home network, but they not allow us to obtain fine-grained information. We are currently developing a version of WTF that would perform continuous monitoring. The next section describes the data collection and processing that WTF currently performs.

3.2 Data Collection

WTF collects the following measurements:

- `pcap` *traces of connections.* We collect tcpdump traces from both the WAN and two wireless monitor interfaces simultaneously. The WAN interface traces give us information about TCP connections and IP packets flowing through the access point, while the wireless interfaces capture radiotap headers [23] to obtain per-frame information about: the source and destination stations, bitrate used for each frame, and whether the frame was retransmitted. The retransmission bit is set if the frame was retransmitted at least once; this does not give us information about how many times a frame was retransmitted.

- *Connection tracking information from Network Address Translator (NAT) module.* To obtain information about the end point of TCP connections inside the home, we collect a snapshot of the conntrack file that has the mapping of WAN ports to LAN IP addresses and ports.

- *ARP information.* This provides the device MAC ID to IP address information of end points inside the home.

- *Per-client 802.11 information.* Depending on the end-host driver, radiotap may not have the MCS (Modulation and Coding Scheme) information for received frames; this means that we cannot use that to extract the frame rates of received frames. We noticed this in only a few hosts, and in order to get around the problem, WTF samples the instantaneous state of each client connected to the access point over 802.11 using the `iw` command every 100 ms. This gives us the instantaneous transmission and reception rates to each client. WTF stores the average and standard deviation of all sampled values in one 15-second iteration.

WTF processes this data locally on the router as follows. First the WAN `pcap` traces are processed to extract timestamps of arriving packets, and information about individual flows (using `tcptrace` [1]). particularly the number 3dupacks, the RTT on either side of the access point, and the number of packets in each connection. Because of the location of the access point, the RTT is broken down into the latency between the access point and either end points. The RTT information is obtained by tracking packets and the corresponding ACK. WTF then processes the radiotap traces to obtain the source and destination MAC addresses and the frame control bits of each frame.

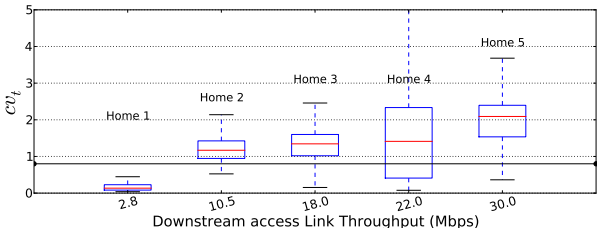


Figure 9: *The distribution of cv_t for 5 homes for which we explore case studies in more detail. Generally, cv_t increases as access link throughput increases because the access link is a bottleneck less often. However, the value of cv_t depends on the quality of the access link in the home network; homes with poor wireless connectivity can have lower cv_t even if the quality of the wireless link is also poor.*

Home	Downstream (MBps)	Characteristic	Downstream Access	Wireless
1	2.8	Slow access, poor wireless	95%	92%
2	10.5	Moderate access, poor wireless	2%	78%
3	18.0	Moderate access	14%	76%
4	22.0	Moderate access	34%	79%
5	30.0	App/End-host bottleneck	9%	15%

Table 3: *Percentage of time WTF detects pathologies in either the downstream access link or the home wireless network.*

WTF anonymizes all IP addresses and MAC addresses completely using SHA-256 and a per-router secret salt as the data is collected on the router. Private information is never stored, and it never leaves the router. This pre-processed data is uploaded to the server and deleted from the router. The data is stored in a database where the diagnosis and longitudinal analysis portions of WTF reside. *All aspects of this study have been reviewed and approved by our university institutional review board (IRB).*

The server sanitizes the timing data before computing the coefficient of packet inter-arrival time, cv_t. Specifically, in our analysis, we only consider cases where we see traffic rates of at least 100 packets per second. For each of these cases, we compute the average and the standard deviation of the inter-packet arrival. We then eliminate all delays that exceed the average plus two standard deviations and recompute the average and the standard deviations again. This step eliminates outliers involving a burst of packets of duration less than one second followed by packet arrivals at slower rates.

4. CASE STUDIES

We now use WTF to explore its behavior in five home networks, and to better understand what gives rise to various conditions in real home networks. Table 3 shows the characteristics of the homes that we selected for our case studies. These characteristics, particularly for wireless, depend on the parameters we choose. However, we tested it with different

parameter settings for RTT latency and normalized throughput and got very similar numbers, suggesting our thresholds are fairly robust.

The homes represent a range of conditions, and we were able to independently validate some of the findings of WTF by talking to users and taking more more detailed measurements where necessary. Section 5 describes our aggregate results across 30 homes across North America over several days. In this section, we focus on WTF's behavior in these five homes with different operating regimes, to provide better confidence in our aggregate results and to allow us to explore some "war stories" from real home network deployments.

Overview: how cv_t relates to access link throughput. Figure 9 shows the values of the coefficient of variance of packet inter-arrival time, cv_t. The figure also shows a horizontal line at 0.8, above which WTF determines that the access link is the bottleneck. The access links for these five homes have a range of downstream through throughput varies from 2.8 Mbps to 30 Mbps. The boxes in the figure represent the inter-quartile range of the cv_t values, while the whiskers represent the 10^{th} and the 90^{th} percentile values. The figure shows that the low throughput home (Home 1) almost always has low cv_t, which confirms the expectation that the usage in this homes almost always saturates the access link, and that the wireless is rarely the bottleneck.

Figure 9 also shows that, in general, cv_t increases as the access link throughput increases: as the access link throughput increases, the wireless has a higher chance of being the bottleneck. The median values for the 22 Mbps and the 30 Mbps homes are above 1, indicating that most of the time the access link is not the bottleneck. Surprisingly, Homes 2 and 3 almost never saturate the downstream access link.

Home 1: Low capacity access link, poor wireless We first explore WTF's measurements in a network that has low downstream throughput on the access link. As expected, the cv_t is low because the access link is often the bottleneck in this home. This trend confirms our intuitive expectation, but we also performed additional measurements to verify these findings. In addition to WTF's measurements, we also perform active throughput measurements about every two hours. Over the period of this study, the access link in Home 1 sees an average downstream throughput of about 2.75 Mbps, with a standard deviation of 150 Kbps—a slow, but extremely stable access link. Saturating the access link requires only about 208 packets a second, assuming 1500-byte packets. We assume that in cases where we see at least 80% of this packet rate per second that the access link is saturated; in these cases, we expect cv_t to be low. Indeed, in nearly 1200 cases where we infer that the access link is the bottlenecked based on observed packet rates, WTF correctly diagnosed all but two of those cases.

Table 3 also indicates that WTF suggests that this home experiences problems in its wireless network a large fraction of the time. Figure 10 plots the upstream retransmission rates (from the client to the AP); WTF observes a high a number of retransmissions. We visited this home network and determined that the access point is about 5–8 meters away from the location where the occupant typically uses his wireless laptop, and that there were multiple walls in between the access point and the laptop. This user also sees fewer retransmissions on the downstream link between the AP and his laptop, perhaps because the AP's radio is more powerful than the client's. Still, despite the fact that the user experiences such poor wireless connectivity, the wireless network is often not the bottleneck in his home because the access link also has such low capacity.

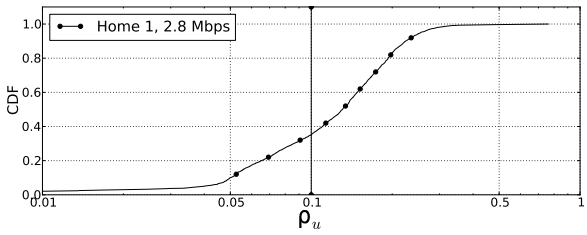


Figure 10: *CDF of ρ_u for Home 1 shows that retransmissions between clients and the access point are greater than 0.1 (10% of frames) nearly 60% of the time.*

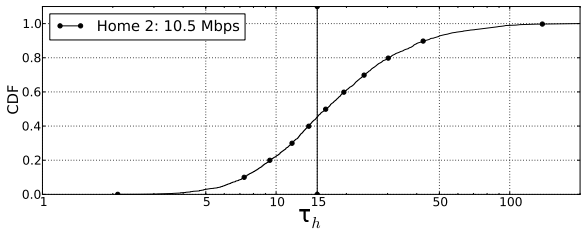


Figure 11: *CDF of τ_h for Home 2 shows that RTT between the access point and clients in the home network exceeds 15 ms about 50% of the time.*

Home 2: Moderate capacity access link, poor wireless. This home has an access link with a downstream throughput of 10.5 Mbps. The access point has also has 802.11n enabled, which might suggest that the wireless link should not typically introduce a bottleneck. Surprisingly, however, WTF found that the access link for this home is almost never saturated! To investigate this further, we visited this home and ran `iperf` between the access point and the client and confirmed that the throughput of the wireless link is approximately 10 Mbits/s; thus, the wireless network in this home network is almost certainly introducing a bottleneck.

WTF also observes high values of upstream and downstream retransmission rates (ρ_u and ρ_u), and TCP round-trip times on the wireless link (τ_h) of greater than 15 ms more than 50% of the time, as shown in Figure 11. Our visit to this home found that the user's wireless access point was indeed located in a closet in the far corner of a 1500-square foot apartment. Further, we found that this home network had tens of devices connected using the access point, exclu-

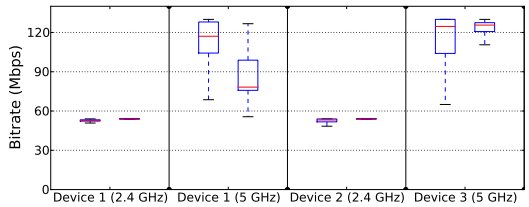


Figure 12: *Range of bitrates for each device in Home 3. For each device, we plot the upstream bitrate on the left, and the downstream bitrate on the right. Over 80% of the measured values are from Device 1 (on 2.4 GHz), which is restricted to a maximum rate of 54 Mbps. Though it is quite steady, it could still bottleneck an 18 Mbps access link.*

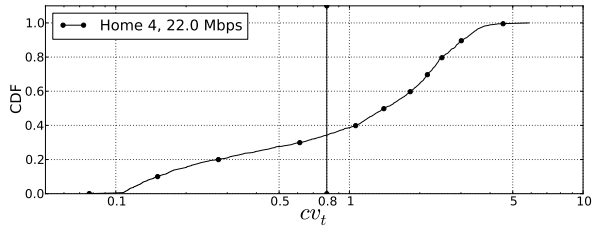


Figure 13: *CDF of cv_t for Home 4. The access link is saturated nearly 40% of the time.*

sively using the 2.4 GHz wireless band, which is likely to face more interference than the 5 GHz channel (particularly for this home, which is located in an apartment complex and within range of approximately 30 other access points). We repeated the test we ran in Home 1 involving packet rates and link saturation and determined that the access point sees a packet rate that is sufficient to saturate 80% of the access link only 20 times out of nearly 1,900 measurements; our measurements confirm WTF's finding that the wireless network is such a problem in this home that the access link is almost never saturated.

Home 3: Moderate capacity access link, mostly 802.11g devices. Home 3 has an 18 Mbps access link. Figure 9 indicates that the access link is not the bottleneck for this user most of the time. WTF also indicates that the wireless is a bottleneck 76% of the time. Upon further investigation of this home network, we discovered that this particular user has devices that do not have 802.11n enabled, which means that these devices cannot achieve a wireless bitrate of more than 54 Mbps. Because the *maximum* TCP throughput achievable over a 54 Mbps 802.11g channel is about 25 Mbps under optimal conditions, it is possible that the wireless is the bottleneck, given that the access link at 18 Mbps. So, though we see from Figure 12 that wireless bitrates are very stable, we also saw that the local TCP RTTs are very high in this network; nearly 90% of medium to large TCP flows (more than 100 packets) saw an average TCP RTT between the access point and the client of more than 15 ms. This effect is pronounced usually for large flows as the wireless bottleneck builds up so we might not see this indicator for shorter flows.

Home 4: Moderate access link, moderate wireless Home 4 has a similar access link capacity as Home 3, but the characteristics of its wireless network are much different. WTF finds a high cv_t value: Figure 13 shows the CDF of cv_t for this home; the figure shows that the access link introduces a bottleneck only about 40% of the time, but also reveals wireless problems nearly 80% of the time. We studied the conditions in this home carefully and confirmed using the packet-rate analysis that we ran in other homes that when the access link is near saturation, cv_t is low. As in other homes, we also measured the wireless throughput from the AP to a device in the home network using iperf, which reported a throughput of 65 Mbps. At times, the wireless is clearly not the bottleneck at least some of the time, which is confirmed by low values of cv_t; but there exist other times when the wireless performance introduces a potential bottleneck, or there isn't sufficient demand on the network.

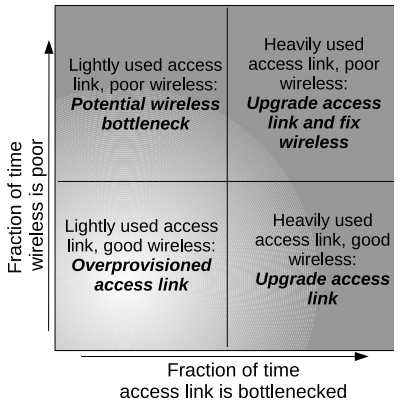
Home 5: High capacity access link, low application demand Finally, we analyze Home 5, which has a 30 Mbps access link. This network almost never saturates the access link; the home also has a good wireless network: WTF detects wireless issues only 13% of the time. In this home, we performed iperf tests from the AP to the most commonly used device in the home. Our tests confirm confirm that the throughput between the AP and the client is more than 60 Mbps. Therefore, we expect applications in the home typically do not generate sufficient demand to saturate either the access link or the wireless network. We asked the user of this home network about his network usage and, indeed, he confirmed that he rarely uses the network heavily. (Apparently, this user knows how to set up a wireless network, but is also paying too much for his ISP service plan!)

5. A GLIMPSE INTO HOME NETWORKS

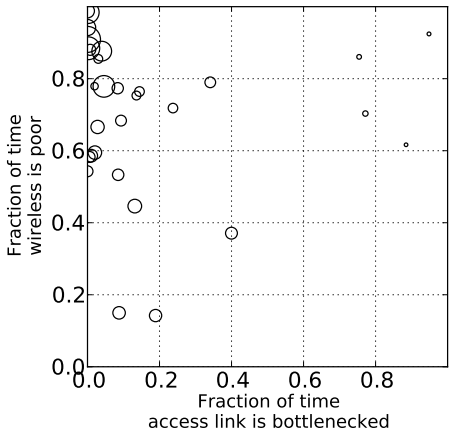
A typical home user can typically only report their experience with the performance of various applications in his or her home network but has no idea whether those problems are caused by problems with the home network or the Internet service provider. The default assumption that users often make is that the problem lies with their ISP (an assumption that costs ISPs millions of dollars) or that it is simply time to buy a faster service plan. However, in many cases, simply moving the wireless access point might significantly improve the performance of their home network [12, 13].

5.1 Before buying a faster service plan... move the router!

WTF's holistic analysis of both the access link and the wireless network can help users understand the state of their home network. For instance, a heavily used access link that is bottlenecked most of the time, coupled with good wireless performance, might suggest that upgrading to a higher service plan may result in better performance, while an access



(a) *Taxonomy and decision matrix.*



(b) *Prevalence of pathologies in 30 homes. Each circle represents one home (circle area is proportional to downstream throughput).*

Figure 14: *Prevalence of performance problems in the deployment*

link that is rarely bottlenecked, coupled with poor wireless performance, might suggest that the user should fix the wireless network to fully utilize the network.

As a first step towards understanding where performance problems truly lie in home networks, we deployed WTF in 30 homes to shed light on the frequency of various pathologies in a range of different home networks. Table 4 summarizes our deployment and the characteristics of the home networks in this deployment.

Figure 14a shows the decision matrix we use to evaluate the homes: good wireless performance with low access link utilization suggests a lightly used network (and the possibility of even downgrading the service plan without adverse effects). High utilization and a poor wireless suggests that the user's time might be well spent optimizing access point placement (or replacement!). Figure 14b places all the homes into Figure 14a's decision matrix. The size of the circle is proportional to the downstream throughput of the access link for that home. The results show that *most homes in our deployment have wireless problems most of the time, and are likely bottlenecked by the wireless network.* All home networks are affected by wireless problems, except those with access links whose downstream throughput is less than 10 Mbits/sec. (We observed a few homes with moderate access links and good wireless that do not make heavy use of the network.)

Number of Households	30
Duration	9—21 days
Devices (2.4 GHz)	215
Devices per house (2.4 GHz)	1–23
Active devices (2.4 GHz)	104
Devices (5 GHz)	62
Devices per house (5 GHz)	1–7
Active devices (5 GHz)	37

Table 4: *We deployed WTF in 30 households across North America.*

5.2 How common are wireless pathologies?

We now attempt to better understand the nature of wireless pathologies in homes when they do arise. We note that we are effectively only looking at *symptoms*, rather than underlying causes. For example, we can study the prevalence of various pathologies, but we cannot (yet) explain why we observe them (*e.g.*, whether problems exist due to noisy channels, contention, hidden terminal problems, etc.). We leave a deeper analysis of underlying causes of wireless pathologies in home networks to future work and report only on the prevalence of various symptoms.

What bitrates are observed in home networks? WTF measures per-device bitrates by sampling the output of `iw` every 100 ms whenever WTF runs (*i.e.*, 15 seconds every five minutes) and uploads the results to the server. Figure 16 plots the median of the average bitrate over all devices; we categorize the devices based on whether they are using 2.4 GHz or 5 GHz (Figures 16a and 16b, respectively). The figure shows that upstream bitrates are almost always lower than the the downstream bitrates, which may be due to the fact that access point radios are typically higher quality than client radios. Downstream rates are better for the 5 GHz devices than the 2.4 GHz radios, but there is also more difference between the upstream and the downstream bitrates in 5 GHz band: 50% of 5 GHz devices see median downstream bitrates above 100 Mbps downstream, but 80% see less than 60 Mbps upstream. By comparison, only 25% of 5 GHz devices see median bitrates above 100 Mbps downstream, but only 60% see less than 60 Mbps upstream. Poorer quality client radios might cause more problems in the upstream direction in the 5 GHz band because of stronger signal attenuation.

What are typical TCP round trip times on home wireless links? We used WTF to study the TCP RTTs for all downstream flows with more than 100 packets, across all homes. Figure 18 plots the CDF of the average RTT between the access point and a wireless client, and between the access point

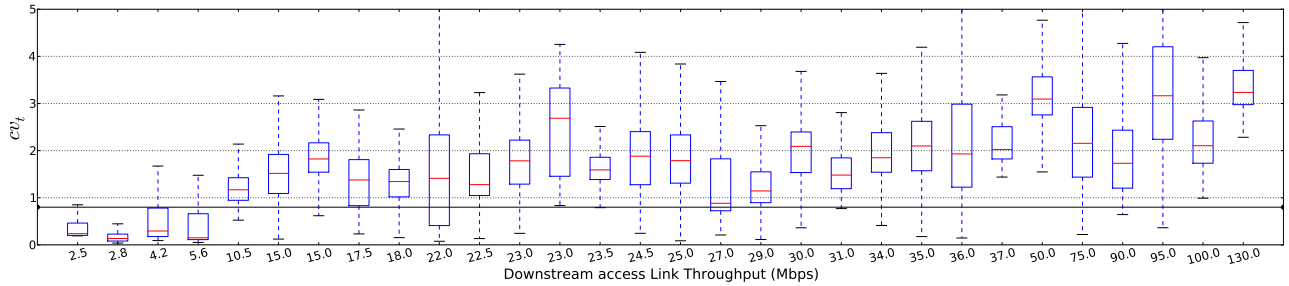
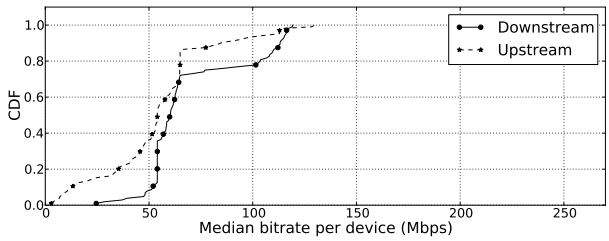
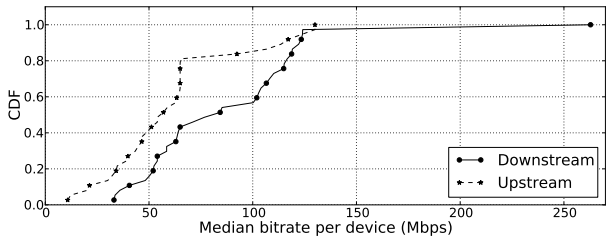


Figure 15: *cv_t values for all homes in the deployment; values below the horizontal line indicate consistent access link bottlenecks. None of the home networks whose access links have downstream throughput greater 27 Mbps experience a significant access link bottleneck.*

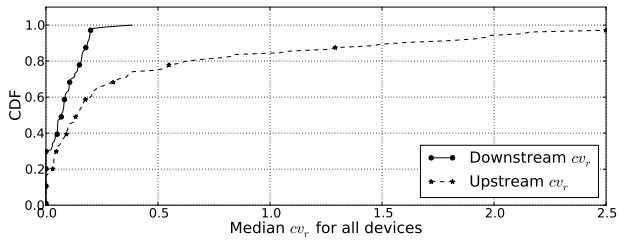


(a) *Median bitrates of all the devices on 2.4 GHz over the deployment.*

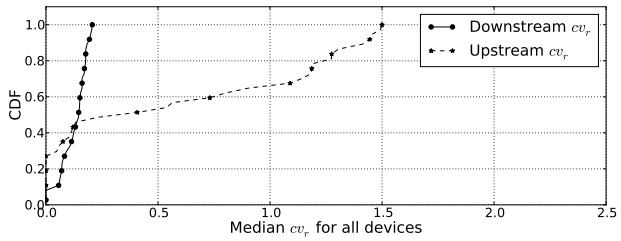


(b) *Median bitrates of all the devices on 5 GHz over the deployment.*

Figure 16: *Distribution of wireless bitrates for devices in both the 2.4 GHz and 5 GHz spectrums, for all devices in the deployment. Downstream bitrates are higher than upstream bitrates on both spectrums.*



(a) *20% of 2.4 GHz devices have high median upstream bitrate variation*



(b) *50% of 5 GHz devices have high median upstream bitrate variation*

Figure 17: *Variation of upstream and downstream wireless bitrates (cv_r) across devices in the 2.4 GHz and 5 GHz bands.*

and the server with which the home user is exchanging traffic. The median RTT on the local wireless network is about 25 ms, which is nearly as high as the median RTT that users experience between their access point and the services they are accessing, 40 ms! This finding suggests that *the RTT introduced by the wireless network may be a significant fraction of the end-to-end RTT* (at least in North America where our current deployment is located).

This finding is particularly significant in light of the many recent efforts by service providers to reduce latency to end-to-end services with myriad optimizations and careful placement of content. In addition to the significant attention that is already being paid to optimizing wide-area performance and host TCP connection settings, it may well be worth spending effort to improve home wireless network performance. The next steps should be to understand the underlying causes of this latency, which may be due to channel contention, retransmission, or buffering delays caused by a bottlenecked wireless channel.

What TCP loss and RTT along end-to-end paths do home users experience for the services they use? WTF's ability to analyze properties of TCP connections from real user traffic in deployed home networks also provides a unique opportunity to understand the nature of wide-area performance that users experience for real services. Although there has been much work concerning wide-area performance, and even some work that aims to understand the performance of access networks using active measurements, to date there have been no studies exploring the wide-area connectivity that users actually experience for the applications and services that they are using.

Figure 18 shows that, in general, users experience low round-trip times to the services that they access: Only 20% of the connections exceed 100 ms RTT from the access point to the server. We also saw that that loss is generally low: only about 20% of TCP connections experience non-negligible loss, and fewer than 10% of connections see more than 0.1%

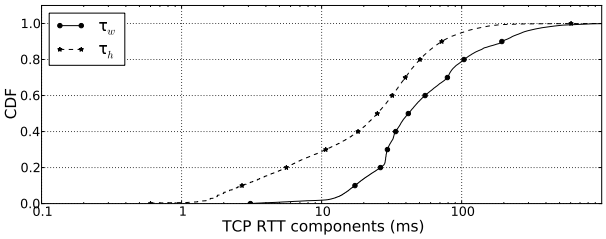


Figure 18: *TCP RTT over wireless is high compared to the RTTs between the access point and the server. This could cause significant performance degradations.*

3dupacks (not shown). In conclusion, the wide-area connectivity properties for the users in our deployment are much less likely to cause performance problems than the user's home wireless link! Although a more widespread deployment of WTF is necessary before one can start drawing general conclusions about where problems lie "most of the time", our deployment certainly suggests that optimizing the performance of home networks deserves more attention.

5.3 How common are access link bottlenecks?

Figure 15 shows the coefficient of variance for packet inter-arrival time on the access link cv_t for all 30 homes in our deployment. The box plot shows the inter-quartile range of the cv_t values for cases when there the traffic on the access link exceeds 100 packets/sec (*i.e.*, when the network is not idle). We observe that *none of the homes with downstream throughput greater 27 Mbps experience a significant access link bottleneck* (which we define as having the 25th percentile value of cv_t falling below the bottleneck detection threshold). We also observe two other features: First, cv_t generally increases as access link speed increases, again confirming WTF's heuristic. This result makes sense: With higher downstream throughput, the likelihood of the access link being bottlenecked with traffic reduces, and the likelihood of the wireless being the bottleneck increases. Second, we observe large variations in cv_t, even among similar access links. This variation results from varying wireless conditions and usage patterns across households: The home with the 18 Mbps access link almost never experiences an access link bottleneck, whereas users in the home with a 22 Mbps access link experience a bottleneck on the access link almost half of the time.

6. RELATED WORK

Although much work exists on detecting both performance bottlenecks and wireless pathologies, none of the prior tools to date have been applied in a *holistic* fashion to isolate problems that users experience in home networks. We believe that this paper presents the first study of the extent and nature of performance problems that real users experience in home networks, and to what extent these problems are caused by problems inside or outside the home. We take a brief look at the different approaches taken towards network diagnosis in both general and 802.11 settings.

A lot of work exists on available bandwidth and bottleneck detection; much of it employs active detection techniques and requires one or both endhosts to probe the network. PathNeck [14, 15] is an active probing tool developed to accurately locate the bottleneck links using Recursive Packet Trains to estimate available bandwidth. Other tools [21, 28, 29] solve similar problems. Similarly, many tools provide estimates of available bandwidth [5, 16, 18, 27]. These techniques are designed to be run from endhosts and can be used as a starting point for diagnosing the problems faced by end hosts in home networks.

Home networks can experience a wide range of performance problems, from misconfigured devices to wireless problems to network neutrality violations. Netprints [3] is a diagnostic tool for home networks solves problems arising due to misconfigurations of home network devices including routers. Significant work has been done on looking at performance degradations due to service i discrimination [10, 11, 17, 31]. Kanuparthy *et al.* [19] develop a tool to detect common wireless pathologies such as low SNR, congestion, and hidden terminals. using both active probes and an additional measurement point within the same wireless network. Many other diagnostic tools used for detecting pathologies in wireless enterprise networks exist [2, 8, 24]. Systems have been developed to exploit specialized hardware or extra monitors to detect the cause of various classes of wireless problems [7, 24–26]. Cooperative techniques exist to diagnose certain classes of problems like hidden terminals and conflict graphs [4, 22].

Our work is different in several ways. First, our study examines wireless networks in 30 homes. To our knowledge, a study of this scale has has not been done before for home networks. Second, WTF uniquely solves a specific problem due to its vantage point in the the middle of the end-to-end path, at the point that separates the home network from the access link. WTF tries to understand performance issues in home networks by being situated on the access point, allowing it to simultaneously determine the characteristics of both the access link and the wide-area path for real user traffic. Third, WTF relies almost entirely on passive techniques to make its inferences. One of WTF's techniques exploits packet inter-arrival times at the access point to determine the location of bottleneck, similar to Katabi *et al.* [20], which uses the entropy in packet inter-arrival time for estimating shared bottlenecks. Biaz *et al.* [6] also use packet inter-arrival, but for distinguishing between different kinds of losses.

7. CONCLUSION

As broadband Internet access proliferates and brings high-speed connectivity into homes, many users' typical Internet experience is defined by the performance that they experience when using their home network. Although there have been extensive studies of wide-area Internet performance and

even studies of access-link performance, to date we have had very little visibility into the "last 50 feet", and how the characteristics of the home network can introduce performance problems for users in home networks. In this paper, we have introduced WTF, a tool that runs on the router in a user's home network, that can provide this much needed visibility to users and ISPs alike. Our results are striking: they suggest that most users who have access links with downstream throughput that exceeds about 10 Mbits/s need not worry about their access link—when these users experience bottlenecks, the underlying cause is most often a poorly performing wireless network.

WTF takes an important first step in home network diagnosis and lays the groundwork for much follow-up work. Our first goal is to develop a version of WTF that can operate online, on unsampled network traffic. A second important extension to WTF involves developing methods that explain *why* various wireless performance problems exist. WTF can tell a user that their home wireless network is performing poorly, but it does not offer any insights into the underlying causes for that poor performance. In addition to working with the Federal Communications Commission and directly with several ISPs to expand our current deployment to a larger set of users, we also plan to develop techniques to better understand the underlying causes of poor wireless performance in home networks.

REFERENCES

[1] tcptrace: A TCP Connection Analysis Tool. `http://irg.cs.ohiou.edu/software/tcptrace/`.

[2] A. Adya, P. Bahl, R. Chandra, and L. Qiu. Architecture and techniques for diagnosing faults in ieee 802.11 infrastructure networks. In *Proceedings of the 10th annual international conference on Mobile computing and networking*, MobiCom '04, pages 30–44, New York, NY, USA, 2004. ACM.

[3] B. Aggarwal, R. Bhagwan, T. Das, S. Eswaran, V. N. Padmanabhan, and G. M. Voelker. Netprints: diagnosing home network misconfigurations using shared knowledge. In *Proceedings of the 6th USENIX symposium on Networked systems design and implementation*, NSDI'09, pages 349–364, Berkeley, CA, USA, 2009. USENIX Association.

[4] N. Ahmed, U. Ismail, S. Keshav, and K. Papagiannaki. Online estimation of rf interference. In *Proceedings of the 2008 ACM CoNEXT Conference*, CoNEXT '08, pages 4:1–4:12, New York, NY, USA, 2008. ACM.

[5] D. Antoniades, M. Athanatos, A. Papadogiannakis, E. Markatos, and C. Dovrolis. Available bandwidth measurement as simple as running wget. In *Proc. of Passive and Active Measurement Conference (PAM 2006)*, pages 61–70. Citeseer, 2006.

[6] S. Biaz and N. H. Vaidya. Discriminating congestion losses from wireless losses using inter-arrival times at the receiver. In *Proceedings of the 1999 IEEE Symposium on Application - Specific Systems and Software Engineering and Technology*, ASSET '99, Washington, DC, USA, 1999. IEEE Computer Society.

[7] Y. Cheng, J. Bellardo, P. Benko, A. C. Snoeren, G. M. Voelker, and S. Savage. Jigsaw: Solving the puzzle of enterprise 802.11 analysis. In *Proc. ACM SIGCOMM*, Pisa, Italy, Aug. 2006.

[8] Y.-C. Cheng, M. Afanasyev, P. Verkaik, P. Benkö, J. Chiang, A. C. Snoeren, S. Savage, and G. M. Voelker. Automating cross-layer diagnosis of enterprise wireless networks. *SIGCOMM Comput. Commun. Rev.*, 37(4):25–36, Aug. 2007.

[9] R. Compton, C.L. Woundy and J. Leddy. Method and packet-level device for traffic regulation in a data network. U.S. Patent 7,289,447 B2, Oct. 2007.

[10] M. Dischinger, M. Marcon, S. Guha, K. Gummadi, R. Mahajan, and S. Saroiu. Glasnost: Enabling end users to detect traffic differentiation. In *Proceedings of the 7th USENIX conference on Networked systems design and implementation*, pages 27–27. USENIX Association, 2010.

[11] Glasnost: Bringing Transparency to the Internet. `http://broadband.mpi-sws.mpg.de/transparency`.

[12] R. Grinter, W. Edwards, M. Chetty, E. Poole, J. Sung, J. Yang, A. Crabtree, P. Tolmie, T. Rodden, C. Greenhalgh, et al. The ins and outs of home networking: The case for useful and usable domestic networking. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 16(2):1–28, 2009.

[13] R. Grinter, W. Edwards, M. Newman, and N. Ducheneaut. The work to make a home network work. In *ECSCW 2005*, pages 469–488. Springer, 2005.

[14] N. Hu, L. Li, Z. Mao, P. Steenkiste, and J. Wang. A measurement study of internet bottlenecks. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, volume 3, pages 1689 – 1700 vol. 3, march 2005.

[15] N. Hu, L. E. Li, and Z. M. Mao. Locating Internet bottlenecks: Algorithms, measurements, and implications. In *Proc. ACM SIGCOMM*, pages 41–54, Portland, OR, Aug. 2004.

[16] M. Jain and C. Dovrolis. Pathload: A measurement tool for end-to-end available bandwidth. In *In Proceedings of Passive and Active Measurements (PAM) Workshop*, pages 14–25, 2002.

[17] P. Kanuparthy and C. Dovrolis. Diffprobe: detecting isp service discrimination. In *Proceedings of the 29th conference on Information communications*, INFOCOM'10, pages 1649–1657, Piscataway, NJ, USA, 2010. IEEE Press.

[18] P. Kanuparthy, C. Dovrolis, and M. Ammar. Spectral probing, crosstalk and frequency multiplexing in internet paths. In *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*, IMC '08, pages 291–304, New York, NY, USA, 2008. ACM.

[19] P. Kanuparthy, C. Dovrolis, K. Papagiannaki, S. Seshan, and P. Steenkiste. Can user-level probing detect and diagnose common home-wlan pathologies. *SIGCOMM Comput. Commun. Rev.*, 42(1):7–15, Jan. 2012.

[20] D. Katabi and C. Blake. Inferring congestion sharing and path characteristics from packet interarrival times. Technical Report MIT-LCS-TR-828, Massachusetts Institute of Technology, 2002.

[21] K. Lai and M. Baker. Nettimer: A tool for measuring bottleneck link bandwidth. In *Proceedings of the USENIX Symposium on Internet Technologies and Systems*, volume 134, 2001.

[22] D. Niculescu. Interference map for 802.11 networks. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, IMC '07, pages 339–350, New York, NY, USA, 2007. ACM.

[23] Radiotap. `http://radiotap.org`.

[24] S. Rayanchu, A. Mishra, D. Agrawal, S. Saha, and S. Banerjee. Diagnosing wireless packet losses in 802.11: Separating collision from weak signal. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages 735 –743, april 2008.

[25] S. Rayanchu, A. Patro, and S. Banerjee. Airshark: detecting non-wifi rf devices using commodity wifi hardware. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, IMC '11, pages 137–154, New York, NY, USA, 2011. ACM.

[26] S. Rayanchu, A. Patro, and S. Banerjee. Catching whales and minnows using wifinet: deconstructing non-wifi interference using wifi hardware. In *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation*, NSDI'12, pages 5–5, Berkeley, CA, USA, 2012. USENIX Association.

[27] V. Ribeiro, R. Riedi, R. Baraniuk, J. Navratil, and L. Cottrell. pathchirp: Efficient available bandwidth estimation for network paths. In *Passive and active measurement workshop*, volume 4, 2003.

[28] S. Saroiu, P. Gummadi, and S. Gribble. Sprobe: A fast technique for measuring bottleneck bandwidth in uncooperative environments. In *IEEE INFOCOM*, page 1, 2002.

[29] S. Savage. Sting: a tcp-based network measurement tool. In *Proceedings of the 1999 USENIX Symposium on Internet Technologies and Systems*, pages 71–79, 1999.

[30] S. Sundaresan, W. de Donato, N. Feamster, R. Teixeira, S. Crawford, and A. Pescapè. Broadband internet performance: A view from the

gateway. In *Proc. ACM SIGCOMM*, Toronto, Ontario, Canada, Aug. 2011.

[31] M. Tariq, M. Motiwala, N. Feamster, and M. Ammar. Detecting network neutrality violations with causal inference. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, pages 289–300. ACM, 2009.